(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日:
2005年10月6日(06.10.2005)

PCT

(10) 国际公布号:
WO 2005/093581 A1

(51) 国际分类号[7]: G06F 12/14

(21) 国际申请号: PCT/CN2005/000368

(22) 国际申请日: 2005年3月24日(24.03.2005)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200410017241.3 2004年3月26日(26.03.2004) CN

(71) 申请人(对除美国以外的所有指定国): 上海山丽信息安全有限公司(SHANGHAI SANLEN INFO SECURITY CO., LTD.) [CN/CN]; 中国上海市黄浦区延安东路700号港泰广场1702-03室, Shanghai 200001 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 覃云川(QIN, Yunchuan) [CN/CN]; 周军刚(ZHOU, Jungang) [CN/CN]; 中国上海市黄浦区延安东路700号港泰广场1702-03室, Shanghai 200001 (CN)。

(74) 代理人: 上海智信专利代理有限公司(SHANGHAI ZHI XIN PATENT AGENT LTD.); 中国上海市肇嘉浜路446号伊泰利大厦10楼, Shanghai 200031 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

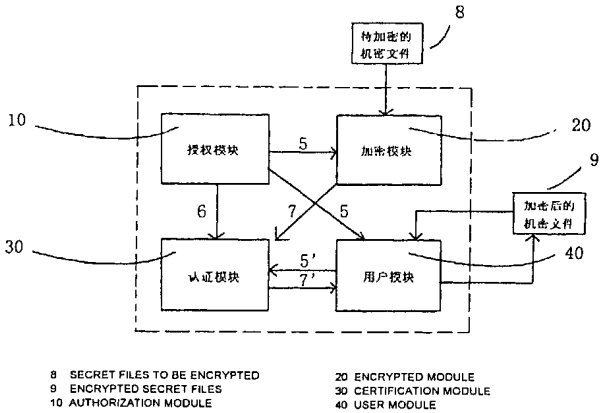
根据细则4.17的声明:
— 关于申请人在国际申请日有权申请并被授予专利(细则4.17(ii))对除美国以外的所有指定国
— 关于申请人在国际申请日有权要求该在先申请的优先权(细则4.17(iii))对下列指定国: 美国
— 发明人资格(细则4.17(iv))仅对美国

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: TITLE: SECRET FILE ACCESS AUTHORIZATION SYSTEM WITH FINGERPRINT LIMITATION

(54) 发明名称: 具有指纹限制的机密文件访问授权系统



(57) **Abstract:** A secret file access authorization system with fingerprint limitation includes an authorization module, a encrypt module and a certification module in the server linked by the programs; and at least one client, each client is provided with a user module, this user module contains a kernel encrypt/decrypt unit embedded in the client operation system kernel, therefore it can realize that access authorization to the secure file is limited by environment fingerprint and time fingerprint Therein an authorization module provides authorization secret key and fingerprint template; an encrypt module receives the input of authorization secret key and secret files to be encrypted and provides the secret key for decryption; a user module receives the authorization secret key and encrypted secret file and provides authorization secret key certification request to certification module; a certification module receives the decrypt secret key and authorization secret key certification request and fingerprint template, and provides certification decrypt secret key to the user to start up kernel encrypt/decrypt unit in the user modules and realizes the operation of reading and writing of the encrypted files.

[见续页]

WO 2005/093581 A1

(57) 摘要

一种具有指纹限制的机密文件访问授权系统包括设在服务器内以程序链接的授权模块、加密模块和认证模块；以及至少一客户机，每一客户机设有用户模块，该用户模块含有一嵌置于客户机操作系统内核的内核加密/解密单元，从而可实现对机密文件的访问授权受到环境指纹或时间指纹的限制。其中授权模块提供授权密钥和指纹范本；加密模块接受授权密钥和待加密机密文件的输入并提供解密密钥；用户模块接受授权密钥和加密机密文件，并向认证模块提供授权密钥认证请求；认证模块接受解密密钥和授权密钥认证请求以及指纹范本，并向用户模块提供认证解密密钥，去启动用户模块中的内核加密/解密单元，实现对加密文件的读出和写入操作。

具有指纹限制的机密文件访问授权系统

技术领域

本发明涉及一种信息安全技术，具体地说，是一种具有环境限制和时间限制的机密文件访问授权的系统。

技术背景

现有的机密文件访问授权系统不具有环境限制和时间限制的机密文件访问授权功能，以文件保险箱技术为例，它在计算机中建立一个加密的存储区以存放机密文件，使用者必须持有授权密钥才能访问该加密存储区中的机密文件。但是，当使用者将该机密文件复制到其它电脑，则任何人无须密钥即可访问。如图 1 所示，其示出 PGPDISK 保护下的文件可以拷贝到未加密的磁盘 B，磁盘 B 可以被带到任何地方，从而失去权限控制。很明显，PGPDISK 的加密/解密没有环境限制，也就是说即使带走的文件是加密的，那么，在另一个地方，只要安装 PGPDISK 软件，也就可以访问该加密文件。

另一种现有技术是机密文件加密技术。被加密的机密文件只有持有授权密钥才能访问。然而，如果该机密文件被持有者转移到非法环境，例如，盗取到家中或盗取到异国它乡，由于持有授权密钥，持有者仍然可以访问该机密文件。换言之，机密文件的授权需要一种“在位授权”机制，即是说，机密文件的授权对象必须在某个职位上或在某种条件下才拥有访问机密文件的权限，一旦授权对象的职位发生改变或者其授权条件消失，他就不应该再持有访问该机密文件的权限。现有访问授权技术无法做到这一点。

发明内容

如上所述，如何克服现有机密文件访问授权系统存在机密文件被非法盗取的缺陷，乃是本发明所要解决的技术问题，为此，本发明的目的之一是将对机密文件的访问授权限制在特定环境内。特定环境可以是单台台式电脑，

单台笔记本电脑，单台掌上电脑,智能电器的计算单元，含有嵌入式计算芯片的设备，以及由上述电脑,电器或设备构成的一定范围的局域网，广域网或互联网及其它数字网络体系。通过本发明提供的技术，管理员可指定授权有效的环境，在该环境之外，指定的机密文件不可访问。

本发明的另一个目的是将对机密文件的访问授权限制在一定时间内，一定时间可以是从当前时间开始计算的一个时间段，例如几小时,几天,几星期,几月等。一定时间还可以是不依赖当前时间的独立时间段，例如星期五上午8:00 到下午 5:30，1 月 1 日到 1 月 31 日等.通过本发明提供的技术，管理员可指定授权有效的一定时间,在指定的有效时间之外，指定的机密文件不可访问。

把上述的本发明目的所确定的环境限制与时间限制进行整合成指纹限制，则本发明的总的目的在于提供一种具有指纹限制的机密文件授权访问系统。

本发明的技术解决方案如下：

根据本发明的一种具有指纹限制的机密文件访问授权系统，包括：一授权服务器，其设有一授权模块，提供一指纹范本和一授权密钥；一加密服务器，其设有一加密模块，接受所述授权模块所提供的授权器钥而产生一解密密钥，以及对待加密的机密文件予以加密而形成加密的机密文件；一认证服务器，其设有一认证模块，接受所述授权模块所提供的指纹范本，和接受所述加密模块提供的解密密钥，以及由客户机送来的请求认证的授权密钥，并判断确认向客户机提供认证的解密密钥；以及至少一客户机，每一客户机内设一用户模块,其在与其相应的客户机的操作系统内核嵌入内核加密/解密单元，接受所述授权模块提供的授权密钥，并将该授权密钥送所述认证模块请求认证，经认证模块返回的认证解密密钥后开启所述的加密/解密单元，对加密的机密文件予以读出和写入操作。

所述授权服务器、加密服务器和认证服务器可以合并成一个系统服务

器，其设有相应的授权模块、加密模块和认证模块；授权模块提供指纹范本和授权密钥；加密模块接受授权密钥并对待加密机密文件予以加密而形成加密机密文件，以及提供解密密钥；认证模块接受所述指纹范本，以及解密密钥，并和所述用户模块连接，接受用户模块送来的授权密钥请求，并予判断而给用户模块返回认证授权密钥与认证解密密钥；

所述授权服务器和加密服务器合并成一个授权与加密服务器，该授权与加密服务器设有授权模块和加密模块，并由授权与加密服务器提供授权密钥、指纹范本、解密密钥以及对待加密机密文件予以加密并形成加密机密文件，并分别与认证服务器的认证模块及客户机的用户模块相联结；

所述授权服务器与认证服务器相结成授权与认证服务器，其内设有的授权模块和认证模块，并分别向加密服务器内的加密模块和向客户机的用户模块提供授权密钥，以及接受客户机的用户模块送来的请求认证其所接受授权密钥，同时返回认证授权密钥和认证解密密钥。

所述的加密服务器与所述的认证服务器结合成一个加密与认证服务器，其内设有加密模块和认证模块；该加密模块接受来自授权服务器所提供的授权密钥而对待加密机密文件予以加密而形成加密机密文件；以及提供解密密钥送该认证模块，再由该认证模块向客户机的用户模块提供认证解密密钥允许客户机进行读出/写入加密机密文件的运作。

进一步，所述授权模块包括：平行设置的口令指纹单元、环境指纹采集单元和时间指纹采集单元，以及后接它们的授权单元，并由该授权单元提供授权密钥和所述的平行设置前三个单元汇集提供指纹范本。所述的指纹范本是一个具有一定长度的二进制数串，其含有口令和环境指纹信息；或含有口令和时间指纹信息；或含有口令、环境指纹和时间指纹信息。所述授权密钥是一个具有一定长度的二进制数串，并可以放入具有授权的实体之中；

所述加密模块包括依次成程序联结的密钥产出单元和加密单元；该密钥产生单元接受授权模块提供的授权密钥后提供解密密钥；该加密单元接受待

加密的机密文件的输入并使用密钥产生单元提供的解密密钥产生加密机密文件或使用授权密钥对待加密机密文件形成加密机密文件；或使用解密密钥和授权密钥来形成加密机密文件；

所述的认证模块包括接受所述授权模块提供的指纹范本而平行设置的环境指纹认证单元、口令指纹认证单元和时间指纹认证单元；以及与它们成双向程序联结的认证接口单元，该认证接口单元还分别接受所述加密模块提供的解密密钥和用户模块送来的请求认证的授权密钥，以及向用户模块提供认证的解密密钥；

所述的客户机用户模块包括依次成双向程序联结的应用程序单元、内核加密/解密单元和输入输出单元；以及接受授权模块提供的授权密钥并将其送入该内核加密/解密单元的授权输入单元；该内核加密/解密单元向所述认证模块提供请求认证的授权密钥和接受由所述认证模块送来的认证的解密密钥；以及该输入输出单元双向连接加密机密文件；该内核加密/解密单元嵌置于所述客户机操作系统内核（操作文件）。更具体地，客户机操作系统为Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server或Linux/Unix或Pocket, Symbian OS, Windows CE 嵌入式操作系统或 Mac OS 或 Sun OS, Novell netware 及其它服务器或网络操作系统。所述应用程序单元的程序可以是Microsoft Office 及其组件或其它桌面应用程序或嵌入式应用程序。

如上所述，本发明的信息安全比现有技术有着实质性的提高，其对机密文件的访问授权受到环境限制和时间限制。

附图说明

图 1 是现有的 PGPDISK 的加密保护示意图。

图 2 是本发明的环境加密保护示意图。

图 3 是本发明的授权模块结构示意图；

图 4 是本发明的加密模块结构示意图；

图 5 是本发明的认证模块结构示意图；

图 6 是本发明的用户模块结构示意图；

图 7 是本发明的系统结构示意图。

具体实施方式

下面根据图 2～7 给出本发明的较好实施例，并予以详细描述，并结合对实施例的阐述，进一步提供本发明的技术细节，使能更好地理解本发明的技术特征和功能特点，但都是为了说明本发明，而不是用以限制本发明的保护范围。

请参阅图 2，其显示本发明的技术方案的构思，即对所有的 I/O 通道（例如所有的机密文件载体之磁盘，光盘，网络，文件，网页等等）进行加密保护，使得不会有未加密的文件被带走；其加解密必须在指定的环境中进行（环境指纹）认证，因此，即使加密文件被带走，由于在另一个地方（环境）无法获得合法的环境指纹，从而无法通过环境认证，这样，盗用者仍然无法打开使用加密文件。

按图 2 所示的技术构思，提供典型实施例：

如图 3 所示本发明的系统中具有一授权服务器 1 其设有：一授权模块 10，上述授权模块 10 具有平行设置的一口令指纹单元 101、一环境指纹采集单元 102 和一时间指纹采集单元 103、以及一后接它们的授权单元 104。上述口令指纹单元 101 根据指定口令产生具有唯一性和不可复制性的数据作为口令指纹。上述环境指纹采集单元 102 从指定环境中采集具有唯一性和不可复制性的数据作为上述环境的指纹。上述具有唯一性和不可复制性的数据可以是网卡 MAC 地址，可以是硬盘的序列号。上述时间指纹采集单元 103 根据当前时间和管理者指定的时间限制生成具有唯一性和不可复制性的数据作为时间指纹。上述授权单元 104 根据上述口令指纹单元 101 生成的口令指纹，与根据上述环境指纹采集单元 102 采集到的环境指纹，或与根据上述时间指纹

单元 103 生成的时间指纹，生成具有唯一性和不可复制性的授权密钥 5。上述具有唯一性和不可复制性的授权密钥 5 是一个具有一定长度的二进制数串。它可以放入具体的授权实体中。上述授权实体具有的表现形式可以是：密码，电子钥匙，数字证书，加密狗及其它具有防犯非法复制功能的硬件或软件。同时，上述口令指纹单元 101 生成的口令指纹，上述环境指纹采集单元 102 采集到的环境指纹，以及上述时间指纹单元 103 生成的时间指纹，可以合并放入一指纹范本 6。在后面将要讨论的认证模块中，以上述指纹范本与待认证指纹进行比较，从而根据比较结果确定认证结果。上述指纹范本 6 是一个具有一定长度的二进制数串。

如图 4 所示，本发明的系统中具有一加密服务器 2，其设有一加密模块 20，上述加密模块 20 具有一密钥产生单元 201 和一加密单元 202，它们依次以程序联结。上述密钥产生单元 201 使用来自上述授权模块 10 提供的授权密钥 5 产生解密密钥 7。上述加密单元 202 使用上述授权密钥 5 和上述解密密钥 7，或仅使用其中之一，对待加密的机密文件 8 执行加密过程，生成加密后的机密文件 9。上述加密过程可以采用公钥方法，也可以采用私钥方法。上述加密后的机密文件 9 可以公开发布。

如图 5 所示，本发明的系统中具有一认证服务器 3，其设有一认证模块 30。上述认证模块 30 设有平行配置的一环境指纹认证单元 301、一口令指纹认证单元 302 和一时间指纹认证单元 303，以及分别与它们成双向程序联结的一认证接口单元 304。上述环境指纹认证单元 301，上述口令指纹认证单元 302，以及上述时间指纹认证单元 303，分别从上述授权模块 10 提供的指纹范本 6 中取得环境指纹范本，口令指纹范本和时间指纹范本。以及，上述环境指纹认证单元 301，上述口令指纹认证单元 302，以及上述时间指纹认证单元 303，通过上述认证接口单元 304 分别从后面图 6 要描述的客户机 4 送出的送认证的授权密钥 5’中取得待认证的环境指纹，口令指纹和时间指纹。认证过程为，上述环境指纹认证单元 301 比较上述环境指纹范本和上述

待认证环境指纹，并把比较结果返回给上述认证接口单元 304。上述口令指纹认证单元 302 比较上述口令指纹范本和上述待认证口令指纹，并把比较结果返回给上述认证接口单元 304。上述时间指纹认证单元 303 比较上述时间指纹范本和上述待认证时间指纹，并把比较结果返回给上述认证接口单元 304。上述认证接口单元 304 根据上述三个比较结果判断，如果三个结果都是相同则认证成功，否则认证失败。并且只在认证成功的情况下，上述认证接口单元 304 将会把来自上述加密模块 20 提供的解密密钥 7 生成认证的解密密钥 7’送给请求认证的用户模块 40，用户模块 40 方可以此认证解密密钥 7’解密已加密的机密文件 9（参见图 6）。

如图 6 所示，本发明的系统中具有至少一客户机 4，每一客户机 4 设有一用户模块 40。上述用户模块 40 具有依次成程序联结的一授权输入单元 401，和一内核加密/解密单元 402；该内核加密/解密单元 402 分别与一输入输出单元 403 成双向联结，和与一应用程序单元 404 成双向程序联结。上述授权输入单元 401 接受用户输入的上述授权实体，并从上述授权实体中取出其中含有的授权密钥 5,并将该授权密钥 5 传递给上述内核加密/解密单元 402。上述内核加密/解密单元 402 连接上述认证模块 30 之认证接口单元 304，并提交上述授权密钥 5 请求认证。如果认证通过，则从上述认证模块 30 之认证接口单元 304 获得解密所必须的上述认证的解密密钥 7’。上述内核加解密单元 402 系无缝嵌入在操作系统内核及应用程序内核，从而能用上述授权密钥 5 和上述认证的解密密钥 7’对所有读进和写入的上述加密后的机密文件 9 进行加密/解密动作。如果授权无效，则认证必定失败，则上述内核加解密单元 402 不能取得上述认证的解密密钥 7’，从而无法解密上述加密后的机密文件 9，从而使之不可访问。上述操作系统可为 Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server.上述操作系统可以是 Linux/Unix 操作系统；上述操作系统可以是 Pocket, Symbian OS, Windows CE 等嵌入式操作系统；上述操作系统可以是 Mac OS；上述操作系统可以是 Sun OS，Novell

netware 及其它服务器或网络操作系统。上述应用程序可以是 Microsoft Office 及其组件；上述应用程序可以是其它桌面应用程序或嵌入式应用程序。

如上所述，本实施例系统的组成包括：一授权服务器 1，内设授权模块 10；一加密服务器 2，内设加密模块 20；一认证服务器 3，内设认证模块 30；以及至少一客户机 4，每一客户机 4 内设用户模块 40，所述的授权模块 10、加密模块 20 和认证模块 30，以及用户模块 40 它们的连接关系则如图 5 所示，所述的授权模块 10 提供指纹范本 6 送认证模块 30；提供授权指纹 5 分别送加密模块 20 和用户模块 40；加密模块 20 对待加密的机密文件 8 进行加密而形成加密的的机密文件 9，并向认证模块 30 提供解密密钥 7；认证模块 30 接受指纹范本 6、解密密钥 7，以及由用户模块 40 送来的请求认证授权指纹 5'，经确认授权指纹 5' 后向用户模块 40 返回经认证的解密密钥 7' 用户模块 40 获得认证模块 30 送来的认证解密密钥 7' 后使设在客户机 4 的操作系统内核（文件系统）的内核加密/解密单元 402 动作而允许对加密机密文件 9 进行读出和写入。

作为上述实施例的替换，授权服务器 1、加密服务器 2 和认证服务器 3 可以合并而由一只系统服务器来取代，并在该系统工程服务器内设置授权模块 10、加密模块 20 和认证模块 30，它们的内部设置以及相互联结则仍照上述实施例。

当然，也可采用把加密服务器 2 与授权服务 1 合并且分别设置相应的加密模块 20 和授权模块 10，而认证服务器 3 为独立体，并内设认证模块 30。

权利要求

1、一种具有指纹限制的机密文件访问授权系统，包括：

一授权服务器，其设有一授权模块，提供一指纹范本和一授权密钥；

一加密服务器，其设有一加密模块，接受所述授权模块所提供的授权器钥而产生一解密密钥，以及对待加密的机密文件予以加密而形成加密的机密文件；

一认证服务器，其设有一认证模块，接受所述授权范块所提供的指纹范本，接受所述加密模块提供的解密密钥，以及由客户机送来的请求认证的授权密钥，并判断确认提供认证解密密钥；以及

至少一客户机，每一客户机内设一用户模块，其在与其相应的客户机的操作系统内核嵌入内核加密/解密单元，接受所述授权模块提供的授权密钥和加密模块提供的解密密钥，并分别送认证模块请求认证，经认证模块认证后返回认证的授权密钥和认证的解密密钥而开启所述的加密/解密单元，对加密的机密文件予以读出/写入。

2、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于，所述的授权服务器、加密服务器和认证服务器合并成一个系统服务器，其内设置所述的授权模块、加密模块和认证模块。

3、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权服务器和加密服务器合并成一个授权与加密服务器，其内设置所述的授权模块和加密模块。

4、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权服务器和认证服务器合并成一个授权与认证服务器，其内设置所述的授权模块和认证模块。

5、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密服务器和认证服务器合并成一个加密与认证服务器，其内

设置所述的加密模块和认证模块。

6、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述授权模块包括：平行设置的一口令指纹单元、一环境指纹采集单元和一时间指纹采集单元，以及分别与该平行设置前三个单元成双向程序链接的授权单元；该授权单元提供授权密钥；而该平行设置的口令指纹单元、环境指纹采集单元和时间指纹采集单元则汇合提供指纹范本。

7、根据权利要求 6 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权密钥是一个具有一定长度的二进制数串。

8、根据权利要求 7 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权密钥可以放入具有授权实体之中。

9、根据权利要求 6 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的指纹范本是一个具有一定长度的二进制数串。

10、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密模块包括依次成程序联结的密钥产出单元和加密单元；该密钥产生单元接受来自授权模块提供的授权密钥后提供解密密钥；该加密单元接受待加密的机密文件输入并使用密钥产生单元提供的解密密钥而产生加密后的机密文件。

11、根据权利要求 10 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密单元接受待加密的机密文件输入并使用所述授权密钥产生加密机密文件。

12、根据权利要求 10 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密单元接受待加密的机密文件输入并同时使用所述的解密密钥和授权密钥而产生加密机密文件。

13、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述认证模块包括接受所述授权模块提供的指纹范本而平行设置的一环境指纹认证单元、一口令指纹认证单元和一时间指纹认证

单元；以及与它们成双向程序联结的认证接口单元，该认证接口单元还分别接受所述加密模块提供的解密密钥和用户模块送来的请求认证的授权密钥，以及向用户模块提供认证的解密密钥。

14、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述用户模块包括依次成双向程序联结的应用程序单元、内核加密/解密单元和输入输出单元；以及接受授权模块提供的授权密钥并将其送入该内核加密/解密单元的授权输入单元；该内核加密/解密单元向所述认证模块提供请求认证的授权密钥和接受由所述认证模块送来的认证的解密密钥；以及该输入输出单元双向连接加密机密文件；该内核加密/解密单元嵌置于所述客户机操作系统内核。

15、根据权利要求 14 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述客户机操作系统为 Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server 或 Linux/Unix 或 Pocket, Symbian OS, Windows CE 嵌入式操作系统或 Mac OS 或 Sun OS, Novell netware 及其它服务器或网络操作系统。

16、根据权利要求 14 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述应用程序单元的程序可以是 Microsoft Office 及其组件或其它桌面应用程序或嵌入式应用程序。

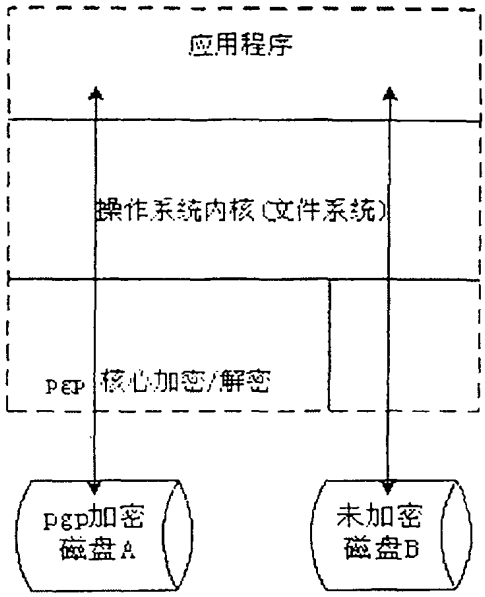

应用程序
操作系统内核(文件系统)
pgp 核心加密/解密
pgp加密
磁盘A
未加密
磁盘B

图1

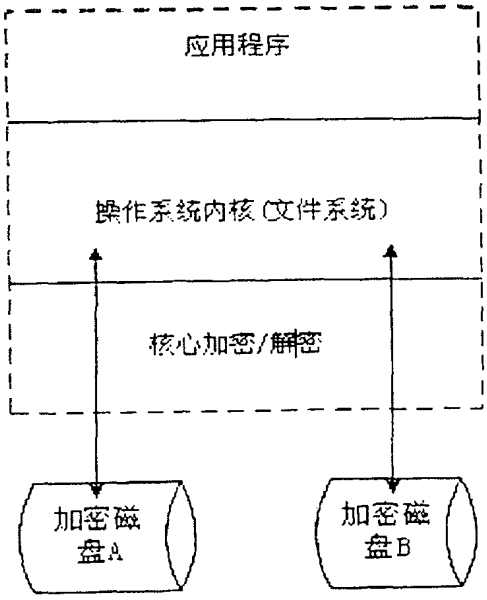

应用程序
操作系统内核(文件系统)
核心加密/解密
加密磁
盘A
加密磁
盘B

图2

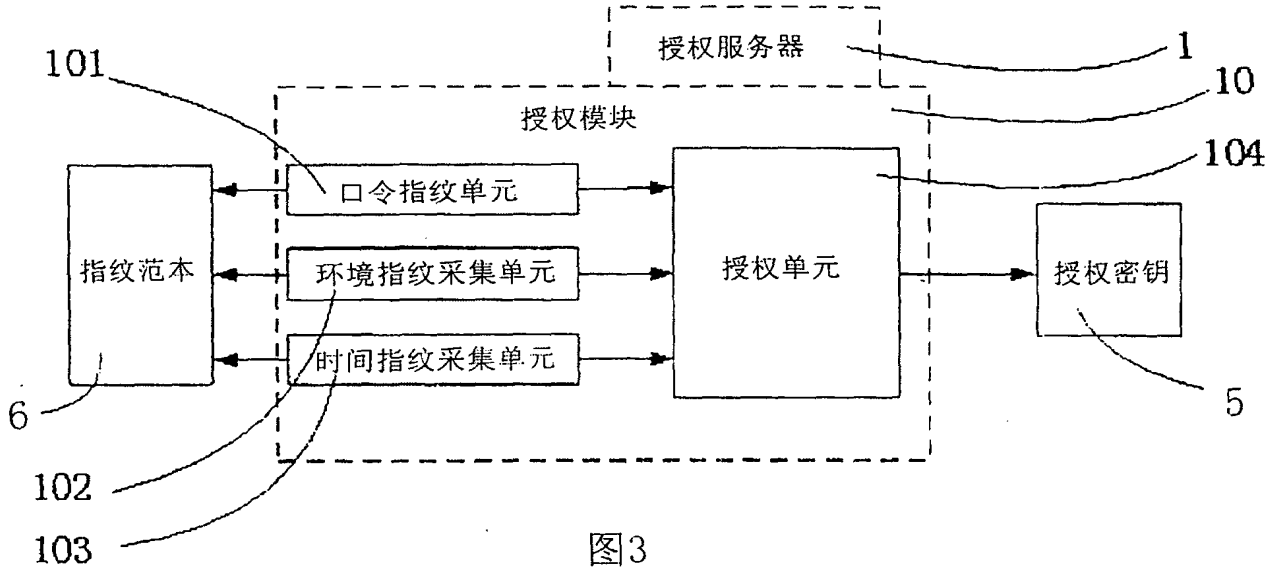

授权服务器
1
101
10
授权模块
104
口令指纹单元
指纹范本
环境指纹采集单元
授权单元
授权密钥
时间指纹采集单元
6
5
102
103

图3

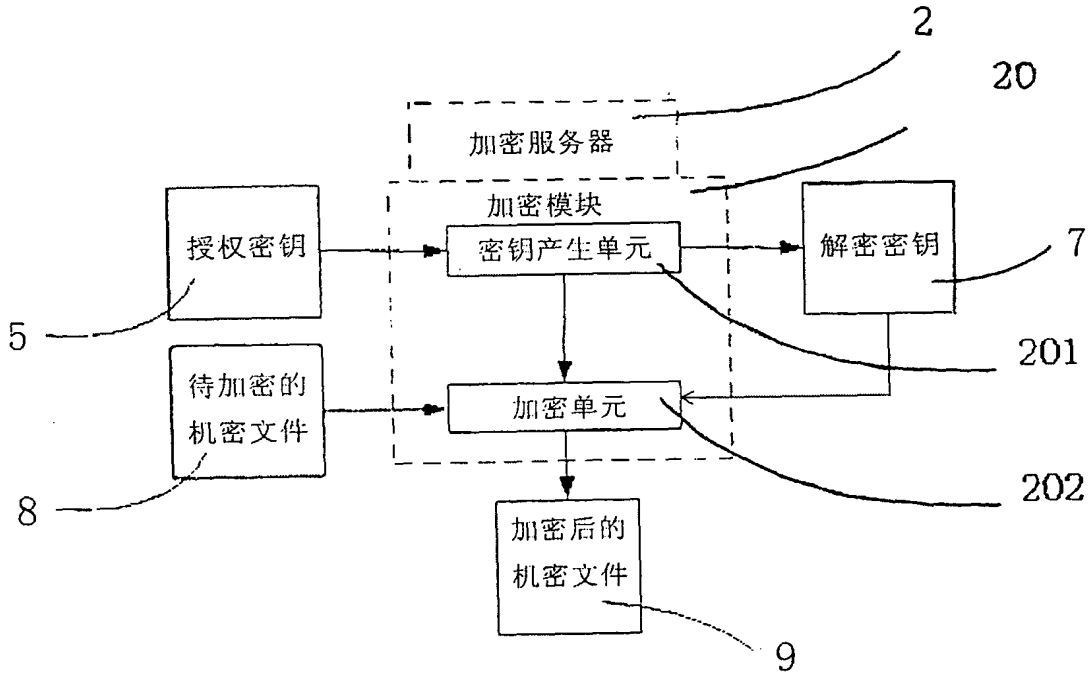

2
20
加密服务器
加密模块
授权密钥
密钥产生单元
解密密钥
7
5
201
待加密的
机密文件
加密单元
202
8
加密后的
机密文件
9

图4

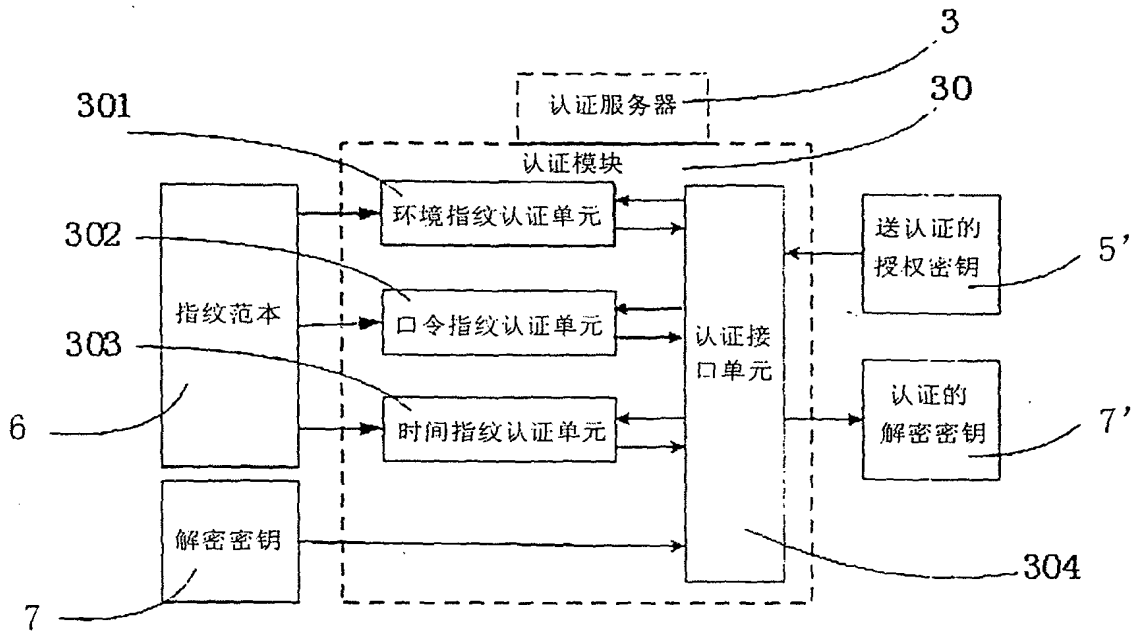

3
认证服务器
30
301
认证模块
环境指纹认证单元
302
口令指纹认证单元
303
时间指纹认证单元
指纹范本
6
解密密钥
7
认证接口单元
送认证的授权密钥
5'
认证的解密密钥
7'
304

图5

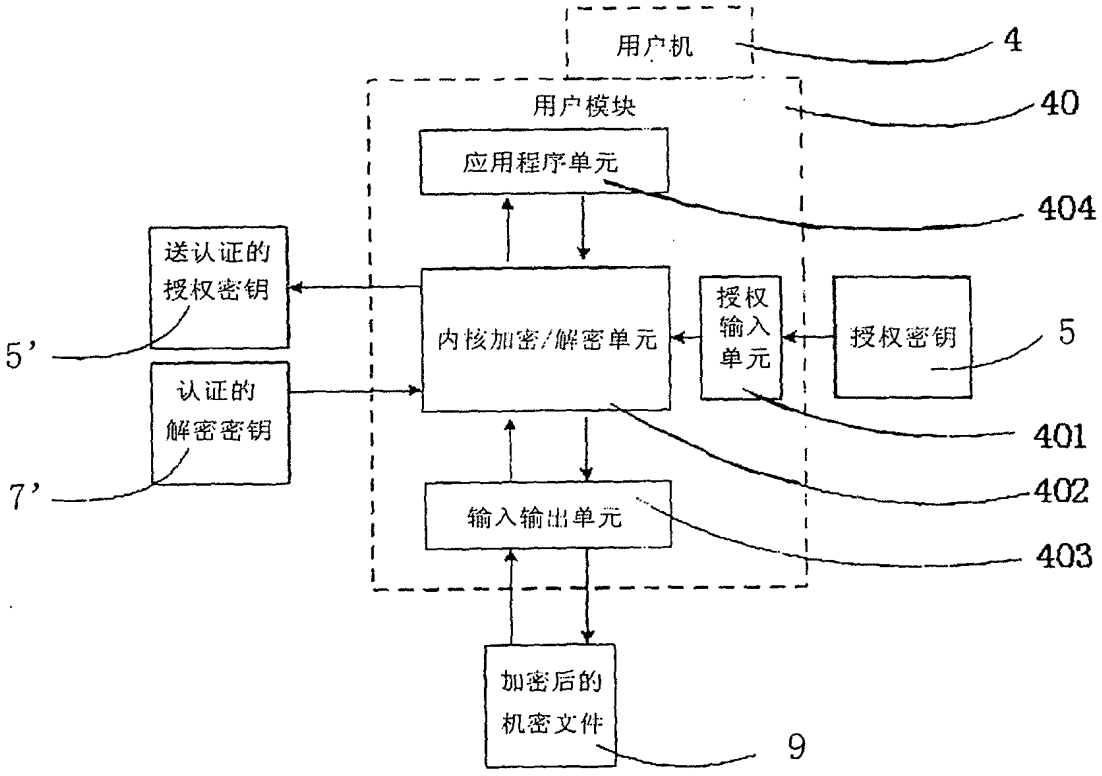

用户机
4
用户模块
40
应用程序单元
404
送认证的授权密钥
5'
认证的解密密钥
7'
内核加密/解密单元
授权输入单元
授权密钥
5
401
402
输入输出单元
403
加密后的机密文件
9

图6

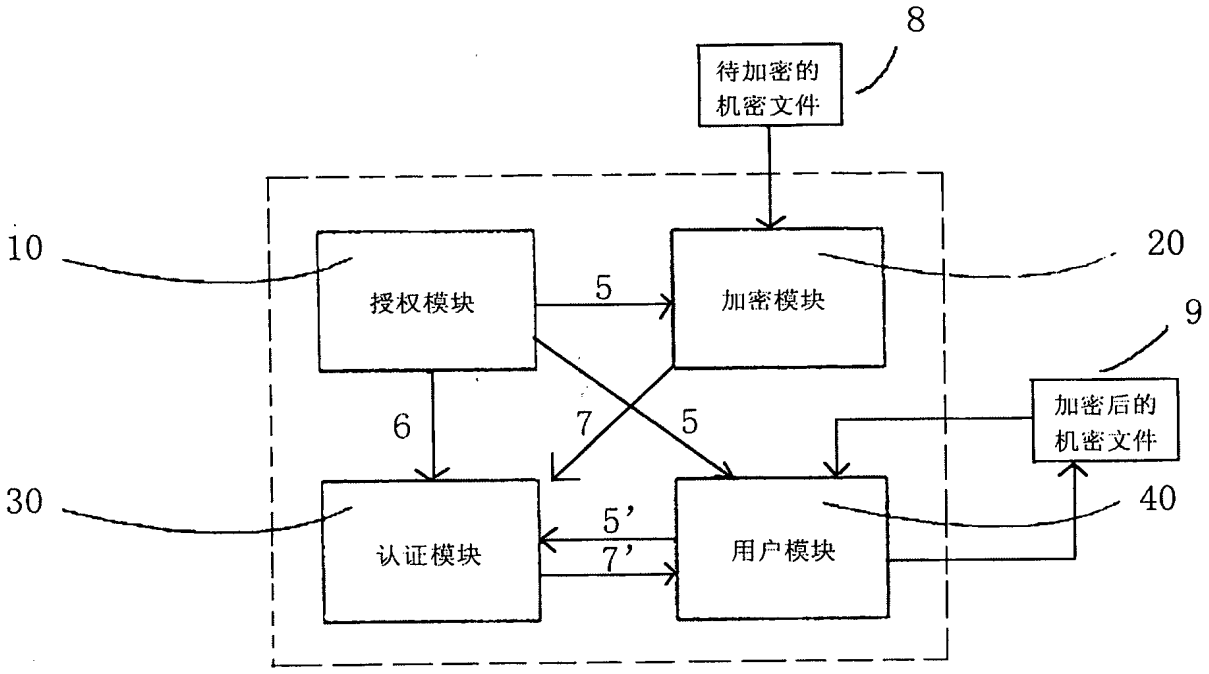


图7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2005/000368

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7] G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7] G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT,WPI,EPODOC,PAJ:encrypt decrypt authorization key secret input fingerprint verify certificate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1405686A (DONGWEICHENG SCI TECHNOLOGY CO LTD) 26.Mar 2003 (26.03.2003) the whole document	1—16
A	CN1324028A (MATSUSHITA ELECTRIC IND CO LTD) 28.Nov 2001 (28.Nov 2001) the whole document	1—16
A	US2003053632A1 (KONINK PHILIPS ELECTRONICS NV) 20.Mar 2003 (20.03.2003) the whole document	1—16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21.Jun 2005 (21.06.2005)	07 · JUL 2005 (07 · 07 · 2005)

Name and mailing address of the ISA/CN	Authorized officer
The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	YUAN, Liying Telephone No. (86-10)62084927

Form PCT/ISA /210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2005/000368

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1405686A	26.Mar 2003 (26.03.2003)	No	
CN1324028A	28.Nov 2001 (28.11.2001)	JP2002033727 A	31.Jan 2002 (31.01.2002)
		EP1154348 A2	14.Nov 2001 (14.11.2001)
		US2001056541 A1	27.Dec 2001 (27.12.2001)
US2003053632A1	20.Mar 2003 (20.03.2003)	EP1449321 A2	25.Aug 2004 (25.08.2004)
		WO03026183A2	27.Mar 2003 (27.03.2003)

国际检索报告

国际申请号
PCT/CN2005/000368

A. 主题的分类

IPC[7] G06F12/14

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[7] G06F H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,WPI,EPODOC,PAJ:encrypt decrypt authorization key secret input fingerprint verify certificate

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN1405686A(东维成科技股份有限公司)26.3 月 2003（26.03.2003）全文	1－16
A	CN1324028A（松下电器产业株式会社）28.11 月 2001（28.11.2001）全文	1－16
A	US2003053632A1(皇家飞利浦电子股份有限公司)20.3 月 2003（20.03.2003）全文	1－16

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：
"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
21.6 月 2005（21.06.2005）	07 · 7月 2005 (07 · 07 · 2005)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 袁丽颖 电话号码：(86-10)62084927

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2005/000368

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1405686A	26.3 月 2003（26.03.2003）	无	
CN1324028A	28.11 月 2001（28.11.2001）	JP2002033727 A	31.1 月 2002（31.01.2002）
		EP1154348 A2	14.11 月 2001（14.11.2001）
		US2001056541 A1	27.12 月 2001（27.12.2001）
US2003053632A1	20.3 月 2003（20.03.2003）	EP1449321 A2	25.8 月 2004（25.08.2004）
		WO03026183A2	27.3 月 2003（27.03.2003）